“STAYING ALIVE”

PASADO – PRESENTE – FUTURO

Dra. Isabel Maassardjian
Facultad de Ingeniería y Tecnologías
Universidad Católica del Uruguay
Mayo 2018
imassardj@ucu.edu.uy

ÍNDICE

Mayo-Julio 2017

- Información crediticia/evaluación de riesgos
- 145.5 millones de consumidores
- Datos personales: nombres, números de seguridad social, fechas de nacimiento, correos electrónicos, datos parciales sobre licencias de conducir
- Acceso a tarjetas de crédito de 209.000 consumidores
- Acceso no autorizado a información personal de determinados residentes de Reino Unido y Canadá

➢ De la intrusión

- Vulneración en el framework de código abierto Apache Struts permitiendo la ejecución remota de comandos, controlando el sistema
- Las aplicaciones web de Equifax fueron hackeadas resultando en una brecha de datos

ELIZABETH WARREN
MASSACHUSETTS
COMMITTEES:
BANKING..

Richard F.Smith

Chairman and Chief Executive Officer

Equifax

Your press release indicates that "the company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases."

- ❑ What does this statement mean?
- ❑ What are Equifax's "core consumer or commercial credit reporting databases“ and how are they distinct from other databases containing personal information maintained by Equifax?
- ❑ Which company databases were accessed by the hackers?
- ❑ What is their function, and why are they not considered to be part of Equifax's "core consumer or commercial credit reporting databases“
- ❑ Has Equifax identified the hackers responsible for the breach, and their country of origin?
- ❑ Prior to July 29, 2017 did Equifax have a plan in place to respond to a large-scale security breach? ……..

» https://www.warren.senate.gov/files/documents/2017_09_15_equifax.pdf

TARGET
A SECURITY NIGHTMARE?
Something to Ponder?

Infosecurity

Mayo 2014

METRO DE SAN FRANCISCO
Noviembre 2016

- BART es el sistema de metro de San Francisco y más de 2.000 equipos del transporte público fueron infectados con un ransomware, comprometiendo las máquinas expendedoras de tickets y el monitoreo en las estaciones, lo que impidió que los viajeros pudieran pagar por utilizar el servicio.

- Se permitió a los usuarios viajar gratis durante ese día.

- Desde la empresa, aseguraron que no se vulneraron los firewall, por lo cual los sistemas de pago de los clientes no se vieron afectados, así como tampoco se accedió a las bases de datos alojadas en sus servidores.

- Los atacantes, solicitaron un rescate de 100 Bitcoin equivalente a unos U$S 73.000 que la empresa se negó a pagar.

- Los sistemas de copias de seguridad le permitió a la empresa seguir adelante, y continuar funcionando los días siguientes, e ir recuperando el servicio poco a poco.

Hotel Romantik
Seehotel Jaegerwirt
Austria (Turrach)
2017

- ✓ Temporada alta - 100% ocupación
- ✓ Cuarto ataque
- ✓ El hotel tiene un sistema informático que incluye tarjetas como llaves para el acceso a las habitaciones
- ✓ El ataque con ransomware logró afectar todas las computadoras del establecimiento, incluyendo el sistema de reservas y el sistema de caja.
- ✓ Los huéspedes no podían entrar en sus habitaciones y las nuevas tarjetas de acceso tampoco podían ser programadas.
- ✓ Rescate de € 1.500 en valor de bitcoin
- ✓ Los atacantes desbloquearon el sistema de registro de claves y los equipos, permitiendo que todo funcionara de forma normal nuevamente
- ✓ Se reemplazó el equipo de cómputos y se adoptaron nuevos estándares de seguridad
- ✓ El hotel reemplazará las cerraduras electrónicas por las que operan con una llave física

- ➢ El hotel Hard Rock en Las Vegas fue blanco de malware en mayo de 2016, que expuso los detalles de los clientes luego de que infectara terminales de punto de venta (POS).

INTERNET DE LAS COSAS

- La Unión Internacional de Telecomunicaciones (193 países y 700 entidades), en el marco de sus Recomendaciones, ha adoptado la siguiente definición:

❖ Internet de las cosas (IoT) [UIT-T Y.2060]: Infraestructura mundial al servicio de la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas gracias al interfuncionamiento de tecnologías de la información y la comunicación (existentes y en evolución)

❖ Web de las cosas [UIT-T Y.2063]: Concepto que se refiere a utilizar IoT para conectar y controlar cosas (físicas y virtuales) a través de la malla mundial multimedios ("world wide web", www)

✓ https://www.itu.int/rec/T-REC-Y.2069-201207-I/es

✓ UIT-T Y.2069, pasó a ser la Rec. Y.4050 el 5/2/2016

DOMÓTICA

- Seguridad
- Confort
- Eficiencia energética
- Línea de iluminación, una cortina motorizada, el riego, la piscina, la calefacción, el aire acondicionado, la alarma, las cámaras, la música
- Potencia ciudades
- Edificios

REFLEXIONES FINALES

- Vulnerabilidad/intrusión en el acceso de los sistemas
- Incidentes de seguridad en IoT
- Concientización
- Privacidad
- Posibles fallos en la red
- Costos

Por su atención

Muchas Gracias!